

# Proactive Dependability Framework for Smart Environment Applications

Ehsan Ullah Warriach, Tanir Ozcelebi, Johan J. Lukkien  
 Department of Mathematics and Computer Science  
 Eindhoven University of Technology  
 Eindhoven, The Netherlands  
 {e.u.warriach, t.ozcelebi, j.j.lukkien}@tue.nl

**Abstract**—Smart environment applications demand novel solutions for managing quality of services, especially availability and reliability at run-time. The underlying systems are changing dynamically due to addition and removal of system components, changing execution environments, and resources depletion. Therefore, in such dynamic systems, the functionality and the performance of smart environment applications can be hampered by faults. In this paper, we follow a proactive approach to anticipate system state at runtime. We present a proactive dependability framework to prevent faults at runtime based on predictive analysis to increase availability and reliability of smart environment applications, and reduce manual user interventions.

## I. INTRODUCTION

A Smart Environment (SE) is a physical space enriched with embedded Information Communications Technology (ICT) and adequate software modules, and aims at creating an intelligent and reliable human-centric environment that facilitates humans to use applications efficiently. Physical components together with middleware components make up a system which provides an infrastructure/platform to build SE applications. With ever-growing complexity and dynamicity of SE systems, there is a need to ensure dynamically that a system is performing all functions according to the given specifications e.g., connectivity, and communication, and maintain sufficient level of system resources e.g., energy (battery), and memory. The adoption of SEs is hindered by the fact that there is a constant need for human (or even expert) intervention and the cost of maintenance of such systems is very high. Thus, dependable systems are required, evolving at runtime to maximize the availability and reliability of SE applications.

A SE system can support various applications. Each application can have different requirements from the underlying system. System normal operation states (from the perspective of an application) are those states that maintain the normal operation of the application according to the given specifications. An application failure is defined as the application not being able to satisfy its defined specifications [?]. For example, in smart lighting, the application state space could be three dimensional: 1) the set of acceptable or desired light settings when users are present, 2) the set of acceptable light settings in the absence of users, and 3) the maximum delay from the time a user enters the room until the time light sources

react. Obviously, the dimensions of the application state can change based on the application's ultimate goal(s). When the application does not satisfy the maximum delay requirement or provides an unacceptable light setting in the presence and in the absence of users, the application is said to be in a failure state. Otherwise it is said to be in a normal state.

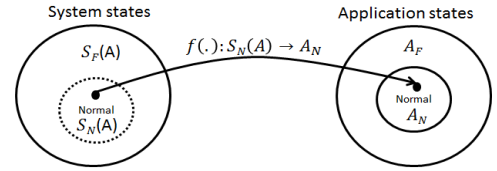


Fig. 1: Mapping from the system states to the application states

Figure 1 shows that the minimum requirements of an application define a boundary around the set of acceptable (or normal operation) states  $A_N$  in its state space, whose dimensions are defined by application quality attributes. The set of all application failure states is  $A_F$ .  $A_F$  and  $A_N$  together span the entire state space of the application. The left side of Figure 1 shows the system state space, whose dimensions are system resources and functions. A given system is said to be in a normal operation state within  $S_N(A)$  with respect to an application  $A$ , if the system in its current state  $S_N(A)$  leads to the normal operation of the application  $A_N$ . The states of the system in  $S_N(A)$  are mapped to (give rise to) the application states in  $A_N$ . In other words,  $f(.) : S_N(A) \rightarrow A_N$ , where  $S_N(A)$  denotes system normal operation states for application  $A$ ,  $S_F(A)$  represents system failure states for application  $A$ ,  $A_N$  represents application normal operation states. When the system state changes from normal to failure (e.g., low Received Signal Strength Indication - RSSI below a certain threshold), this causes the application to fail, i.e., lead the application state to a state outside of  $A_N$  and inside  $A_F$ . The boundary of  $A_N$  is defined by the application specifications. The boundary of  $S_N(A)$  (those system states that map onto  $A_N$ ) may not be known a priori, but can be learned at runtime. As a result, learned system normal and failure states' boundaries of system resources and functions (which are not explicitly defined in the specifications of an application) will be used to predict anomalous events.

In this paper, we present a proactive dependability framework to prevent faults at the system layer regardless of the knowledge of applications. As a result, the SE system will be able to perform its functions with given specifications at hardware and software levels in the presence of an abnormal situation e.g., network node failure, communication error, interference, and battery depletion. We aim for proactive adaptation instead of reactive adaptation mechanisms [?]. Proactive adaptation refers to the case in which the need for adaptation is anticipated, and thus action can be taken to prevent faults that are predicted by the monitoring of the system resources and functions at runtime. We have decomposed the problem of self-learning into two loosely coupled learning problems, to realize the application independent solutions for the proposed dependability framework. First, the system needs to learn at runtime the boundaries of normal and failure states of system resources and functions while running an application. Secondly, the system needs to learn effective adaptation policies for maintaining normal system states.

## II. PROACTIVE DEPENDABILITY FRAMEWORK

The proactive dependability framework consists of four mechanisms: *monitoring*, *analysis*, *adaptation*, and *evaluation* (see Figure 2). The monitoring mechanism is responsible for monitoring the underlying managed system, and providing the current status of system resources  $r_j \in R, j = \{1, 2, \dots, m\}$  and functions  $f_k \in F, k = \{1, 2, \dots, n\}$  to the analysis mechanism at discrete time  $t$ , where time  $t$  refers to a monitoring instance. System resources and functions are monitored by Observable Parameter (OPs)  $v_p \in V, p = \{1, 2, \dots, m\}$ , and  $w_q \in W, q = \{1, 2, \dots, n\}$  respectively. We need to specify what can be and should be monitored and their normal and failure states' boundaries. For example, RSSI provides information about the connectivity of a device, and battery level provides the remaining energy of a device. The monitoring mechanism  $O_{t_i} : R \times F \rightarrow V \times W$  for each time slot  $t_i \in [t_0, t_1, \dots, t_c]$  is defined as  $O_{t_i}(r_1, r_2, \dots, r_m; f_1, f_2, \dots, f_n) = (v_1^i, v_2^i, \dots, v_m^i; w_1^i, w_2^i, \dots, w_n^i)$  where the output is  $(m+n)$  dimensional vector.

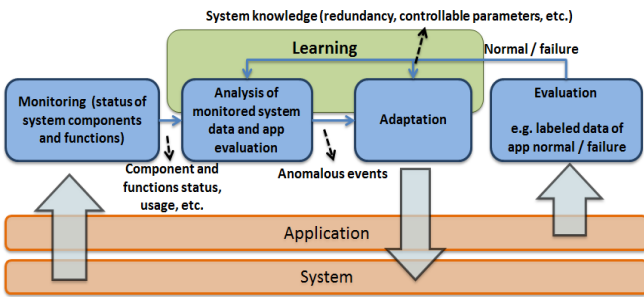


Fig. 2: Proactive dependability framework

The analysis mechanism is responsible to analyze the collected data to identify various anomalous events, and predict faults. First, the system needs to learn a threshold  $\tau$  for each  $v_p \in V$  and  $w_q \in W$ , which denotes the boundary between the system  $S_N$  and  $S_F$  states. A prediction model is used to

predict faults, whenever the value of a system  $r_j \in R$  or  $f_k \in F$  corresponding to  $v_p \in V$  or  $w_q \in W$  is beyond the threshold  $\tau$  (e.g., defined by thresholds of battery level, RSSI level). The outcome of a prediction model is defined by the tuple  $(S, F_{type}, t_{PF}^{min}, t_{PF}^{max})$ , where  $S$  refers to the system resource or function which has expected fault,  $F_{type}$  refers to the type of the predicted fault, and  $[t_{PF}^{min}, t_{PF}^{max}]$  refers to the interval in which the fault is expected.

Adaptation encompasses the mechanisms needed to prevent the predicted faults to keep the system in its normal operation state by autonomously adjusting Controllable Parameters (CPs). The evaluation mechanism checks performance against a set of application requirements to see whether an application is achieving its goals or not. The evaluation mechanism labels the application states with one of two states, namely, normal or failure.

## III. CASE STUDY

The physical low-level infrastructure of SE applications is based on a wireless sensor network (WSN) platform [?]. First, we investigate two important features of a WSN platform, namely, its ability to communicate and its operational lifetime (battery). The operational lifetime of a WSN node is directly related to its energy source and energy consumption. We identified a number of OPs (RSSI, number of direct neighbors, number of received messages, and current energy level) that can be used to monitor the current status of these features, and to assess the current operational state. Similarly, we identified CPs to control dynamically these features (TX power, RX sensitivity, number of TX and RX schedules, round time, sleep/wake intervals, and active local resources) to keep the system in its normal state. An experimental setup is developed to monitor the status of a system function (communication) and resource (battery) by extending the MyriaNed WSN platform with a monitoring mechanism. This platform has been used for various SE applications, e.g., health care, smart homes, environmental monitoring, and intelligent lighting.

## IV. FUTURE WORK

The key issue that we are to address is, how to learn the normal and failure states' boundaries of the system resources and functions at runtime. Another key issue is to develop prediction models for system resources and functions. Further, we need to develop adaptation policies to dynamically prevent the predicted faults using the system knowledge e.g., CPs state boundaries, redundancy, etc. Finally, the most important step is to measure the performance of each adaptation policy with respect to the application availability and reliability, efficient resource management, and the manual interventions from system perspective.